Claims

1. A gateway for connecting an external portion of a network to an internal secured portion of the network wherein the gateway is arranged to identify automatically when a communication session exists between two mobile workstations both of which are connected in the external portion of the network.

2. A gateway as claimed in claim 1, having means for monitoring the source and destination of received packets.

3. A gateway as claimed in claim 1 having secure communication means by which information is transferable securely to the two mobile workstations separately.

4. A gateway as claimed in claim 3 wherein the secure communication means includes a first Security Association with a first mobile workstation and a second Security Association with a second mobile workstation.

5. A gateway as claimed in claim 3 or 4, wherein the gateway is arranged to send, using the secure communication means, an identifier of a second mobile workstation to a first mobile workstation for use as an address in a packet originating from the first mobile workstation and destined for the second mobile workstation

6. A gateway as claimed in claim 5 wherein the identifier of the second mobile workstation is a Home Address.

7. A gateway as claimed in any one of claims 3 to 6, wherein the gateway is arranged to send, using the secure communication means, an identifier of the first mobile workstation to the second mobile workstation for use as an address in a packet originating from the second mobile workstation and destined for the first mobile workstation.

8. A gateway as claimed in claim 7 wherein the identifier of the first mobile workstation is a Home Address.

9. A gateway as claimed in any one of claims 3 to 8, wherein the gateway is arranged to send first security information to the first mobile workstation and second security information to the second mobile workstation using the secure communication means, wherein the first mobile workstation uses the first security information and the second mobile workstation uses the second security information to enable a second secure communication means by which further information is transferable securely between the first mobile workstation and the second mobile workstation without passing through the gateway.

10. A gateway as claimed in claim 9, wherein the second secure communication means comprises Security Associations.

11. A gateway as claimed in any one of claims 1 to 10 wherein the gateway is further arranged to identify automatically when a mobile workstation moves between the internal and the external portions of the network.

12. A network including an internal secured portion which connects, via a gateway to an external portion, the network comprising a plurality of workstations including mobile workstations; the gateway and secure communication means by which information is transferable securely to a first mobile workstation in the external portion of the network via the gateway and by which information is transferable securely to a second mobile workstation in the external portion of the network via the gateway; and information transfer means located within the internal secured portion of the network or within the gateway and arranged to send, using the secure communication means, an identifier of the second mobile workstation to the first mobile workstation for use as an address in a packet originating from the first mobile workstation and destined for the second mobile workstation.

13. A network as claimed in claim 12, wherein the information transfer

means is further arranged to send, using the secure communication means, an identifier of the first mobile workstation to the second mobile workstation for use as an address in a packet originating from the second mobile workstation and destined for the first mobile workstation.

14. A network as claimed in claim 12 or 13 wherein the identifier of a mobile workstation is a Home Address of the mobile workstation.

15. A network as claimed in any one of claims 12 to 14 wherein the secure communication means provides an encrypted communications channel to the first mobile workstation and an encrypted communications channel to the second mobile workstation.

16. A network as claimed in any one of claims 12 to 15 wherein the secure communication means comprises a first Security Association and a second Security Association.

17. A network as claimed in any one of claims 12 to 16 wherein the gateway is arranged to detect a communications session between two mobile workstations which are connected at the external portion of the network.

18. A network as claimed in any one of claims 12 to 17 further comprising:

means for dynamically updating an identifier of the first mobile workstation as it moves within the external portion of the network;

means for communicating the updated identifier of the first mobile workstation to the second mobile workstation; and

means for sending packets from the second mobile workstation to the first mobile workstation using the second secure communication means, wherein the packets are addressed using the updated identifier of the first mobile workstation.

19. A network as claimed in claim 18 wherein the updated identifier is a Care-of-Address.

20. A network as claimed in any one of claims 12 to 19 wherein the network is arranged to use private addresses to communicate within the internal portion of the network and the identifier of the second workstation is a public address.

21. A method of securely routing communications between a first mobile node and a second mobile node of a network including an internal secured portion which connects, via a gateway to an external portion, comprising the steps of:

maintaining a secure communication means by which information is transferable securely to a first mobile node in the external portion of the network via the gateway and by which information is transferable securely to a second mobile node in the external portion of the network via the gateway;

sending an identifier of the second mobile node to the first mobile node using the secure communication means; and

addressing a packet sent from the first mobile node to the second mobile node using the identifier of the second mobile node and routing the packet, using the identifier of the second mobile node, from the first mobile node to the second mobile node, not necessarily via the gateway.

22. A method as claimed in claim 21 further comprising the steps of:

sending an identifier of the first mobile node to the second mobile node using the secure communication means; and

addressing a packet sent from the second mobile node to the first mobile node using the identifier of the first mobile node and routing the packet from the second mobile node to the first mobile node, not necessarily via the gateway.

23. A mobile workstation for connecting to an external portion of a network that includes an internal secured portion connected, via a gateway to the external portion, comprising:

means for using a secure communication means by which information is transferable securely from the internal portion of the network to the mobile workstation via the gateway;

means arranged to receive, via the first secure communication means, an

identifier of another mobile workstation also connected to the external portion of the network; and

means for including the identifier of the other mobile workstation as an address in a packet for transmission to the other mobile workstation.

24. A virtual private network including an internal secured portion which connects, via a gateway to an external portion, the network being arranged to communicate within the internal portion of the network using private addresses and comprising:

a plurality of workstations including mobile workstations;

the gateway;

first secure communication means by which information is transferable securely to a first mobile workstation connected at the external portion of the network via the gateway and by which information is transferable securely to a second mobile workstation connected at the external portion of the network via the gateway; and

information transfer means arranged to send first security information to the first mobile workstation and second security information to the second mobile workstation using the first secure communication means, wherein the first mobile workstation uses the first security information and the second mobile workstation uses the second security information to enable a second secure communication means by which further information is transferable securely between the first mobile workstation and the second mobile workstation without passing through the gateway.

25. A virtual private network as claimed in claim 24, wherein the further information is transferable in packets using public addresses.

26. A network as claimed in claim 24 or 25, wherein the first secure communication means provides an encrypted communications channel to the first mobile workstation and an encrypted communications channel to the second mobile workstation.

27. A network as claimed in claim 24, 25 or 26 wherein the first secure

communication means comprises a first Security Association and a second Security Association.

28. A network as claimed in any one of claim 27, wherein the first Security Association is from the gateway to the first mobile workstation and the second Security Association is from the gateway to the second mobile workstation.

29. A network as claimed in claim 28 wherein the first Security Association is from the internal portion of the network to the first mobile workstation and the second Security Association is from the internal portion of the network to the second mobile workstation.

30. A network as claimed in claim 27, 28 or 29, wherein communications using the first and second Security Associations use addresses which are private.

31. A network as claimed in any one of claims 24 to 30, wherein the second secure communication means provides encrypted communications channels between the first and second mobile workstations.

32. A network as claimed in claim 31 wherein the first and second security information define the encryption/decryption of the encrypted communications channels.

33. A network as claimed in any one of claims 24 to 32 wherein the second secure communication means comprises at least a third Security Association from the first mobile workstation to the second mobile workstation.

34. A network as claimed in claim 33 wherein first and second security information defines at least the third Security Association.

35. A network as claimed in any one of claims 24 to 34, wherein at least a portion of the first security information and at least a portion of the second security information are created within the internal portion of the network.

36. A network as claimed in any one of claims 24 to 35, wherein the gateway is arranged to detect a communications session between two mobile workstations which are connected at the external portion of the network.

37. A network as claimed in any one of claims 24 to 36, wherein the second secure communication means is enabled by the adaptation of databases in the first and second mobile workstations.

38. A network as claimed in any one of claims 24 to 37, further comprising: information transfer means arranged to send, using the first secure communication means, an identifier of the second mobile workstation to the first mobile workstation for use as an address in a packet originating from the first mobile workstation and destined for the second mobile workstation.

39. A network as claimed in claim 38 wherein the identifier of the second mobile workstation is a Home Address.

40. A network as claimed in claim 38 or 39, wherein the identifier of the second mobile workstation is a public address.

41. A network as claimed in any one of claims 24 to 40 further comprising:

means for dynamically updating an identifier of the first mobile workstation as it moves within the external portion of the network;

means for communicating the updated identifier of the first mobile workstation to the second mobile workstation; and

means for sending packets from the second mobile workstation to the first mobile workstation using the second secure communication means, wherein the packets are addressed using the updated identifier of the first mobile workstation.

42. A network as claimed in claim 41 wherein the updated identifier is a Care-of-Address.

43. A method of securing communications between a first mobile node and a second mobile node of a virtual private network including an internal secured portion which connects, via a gateway to an external portion, comprising the steps of:

communicating within the internal portion of the network using private addresses;

maintaining a first secure communication means by which information is transferable securely to the first mobile node in the external portion of the network via the gateway and by which information is transferable securely to a second mobile node in the external portion of the network via the gateway;

sending first security information to the first mobile node using the first secure communication means;

sending second security information to the second mobile node using the first secure communication means;

creating a second secure communication means in the first mobile node, using the first security information in the first mobile node and the second security information in the second mobile node; and

using the second secure communication means, and not the first secure communication means, for transferring further information between the first and second mobile nodes while they both remain in the external portion of the network.

44. A mobile workstation for connecting to a virtual private network that includes an internal secured portion connected, via a gateway to the external portion, and for communicating while in the internal portion using packet addresses which are private to the network, the mobile workstation comprising:

means for using a first secure communication means by which packets addressed to the private address of the mobile workstation are transferable securely from the internal portion of the network to the mobile workstation via the gateway;

means arranged to receive, via the first secure communication means, first security information for enabling a second secure communication means; and

means for using the enabled second secure communication means to

securely receive further packets, addressed to a public address of the mobile workstation, from another mobile workstation also in the external portion of the network.

45. A mobile workstation as claimed in claim 44 further comprising a database and means for modifying the database in response to the received first security information.

46. A mobile workstation as claimed in claim 45 wherein the database includes a Security Association Database (SAD) which is modified to include a new Security Association.

47. A mobile workstation as claimed in claim 46 wherein the database includes a Security Policy database which is modified so that packets for the other mobile workstation use the new Security Association.

48. A virtual private network including an internal secured portion which connects, via a gateway to an external portion, the network being arranged to communicate within the internal portion of the network using private addresses and comprising:

a plurality of workstations including mobile workstations;

the gateway;

secure communication means by which information is transferable securely, without passing through the gateway, between a first mobile workstation connected to the external portion of the network and a second mobile workstation connected to the external portion of the network;

means for dynamically updating an identifier of the first mobile workstation as it moves within the external portion of the network;

means for communicating the updated identifier of the first mobile workstation to the second mobile workstation; and

means for sending packets from the second mobile workstation to the first mobile workstation using the secure communication means, wherein the packets are addressed using the updated identifier of the first mobile workstation and are routed without necessarily passing through the gateway.

49. A network as claimed in claim 48 wherein the updated identifier is a Care-of-Address.

50. A network as claimed in claim 48 or 49 wherein the secure communication means provides encrypted communications channels between the first and second mobile workstations.

51. A network as claimed in any one of claims 48 to 50 wherein the secure communication means comprises a Security Association from the first mobile workstation to the second mobile workstation and a Security Association from the second mobile workstation to the first mobile workstation.

52. A network as claimed in any one of claims 48 to 51 wherein the secure communication means is enabled by databases in the first and second mobile workstations.

53. A method of optimising the routing of secure communications between a first mobile node and a second mobile node of a network including an internal secured portion which connects, via a gateway to an external portion, comprising the steps of:

communicating within the internal portion of the network using private addresses;

creating a secure communication means by which information is transferable securely, without passing through the gateway, between a first mobile node of the external portion of the network and a second mobile node of the external portion of the network;

moving the first mobile node within the external portion of the network;

modifying an identifier of the first mobile node in response to its movement;

communicating the modified identifier of the first mobile node to the second mobile node; and

sending a packet from the second mobile node for reception by the first mobile node, without necessarily passing via the gateway, after addressing it

using the updated identifier of the first mobile and securing it using the secure communication means.

54. A mobile workstation for connecting to an external portion of a network that includes an internal secured portion connected, via a gateway to the external portion, comprising:

means for communicating using private addresses when in the internal portion of the network;

means for enabling and using a secure communication means by which information is transferable securely from the mobile workstation, when in the external portion of the network, to another mobile workstation connected to the external portion of the network without passing through the gateway;

means for receiving an identifier of the other mobile workstation; and

means for sending packets, when in the external portion of the network, to the other mobile workstation using the secure communication means and the received identifier.

55. A mobile workstation as claimed in claim 54 wherein the identifier is a public address.

56. A mobile workstation as claimed in claim 55 wherein the identifier is a Home Address or a Care-of-Address.